

Annual 47 C.F.R. § 64.2009(e) CPNI Certification  
EB Docket 06-36

DOCKET FILE COPY ORIGINAL

Received & Inspected

FEB 27 2009

FCC Mail Room

Annual 64.2009(e) CPNI Certification for 2008

Date filed: 2/24/2009

Name of company(s) covered by this certification: DLS Computer Services, Inc. (dba. DLS Internet Services)

Form 499 Filer ID: 826125

Name of signatory: Sam G. Rozenfeld

Title of signatory: President

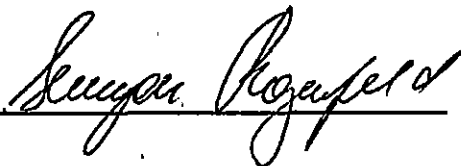
I, Sam Rozenfeld, certify that I am an officer of the company named above, and acting as an agent of the company, that I have personal knowledge that the company has established operating procedures that are adequate to ensure compliance with the Commission's CPNI rules. See 47 C.F.R. § 64.2001 *et seq.*

Attached to this certification is an accompanying statement explaining how the company's procedures ensure that the company is in compliance with the requirements set forth in section 64.2001 *et seq.* of the Commission's rules.

The company has not taken any actions (proceedings instituted or petitions filed by a company at either state commissions, the court system, or at the Commission against data brokers) against data brokers in the past year. Companies must report on any information that they have with respect to the processes pretexters are using to attempt to access CPNI, and what steps companies are taking to protect CPNI.

The company has not received any customer complaints in the past year concerning the unauthorized release of CPNI (number of customer complaints a company has received related to unauthorized access to CPNI, or unauthorized disclosure of CPNI, broken down by category or complaint, *e.g.*, instances of improper access by employees, instances of improper disclosure to individuals not authorized to receive the information, or instances of improper access to online information by individuals not authorized to view the information).

Signed



No. of Copies rec'd 044  
List ABCDE

**DLS Operating Procedures**  
**Implementing 47 C.F.R. Part 64 Subpart U**  
**Governing Use of Customer Proprietary Network information (CPNI")**

**Use of customer proprietary network information.**

DLS Computer Services, Inc. ("DLS") will not use, disclose, or permit access to CPNI for the purpose of providing or marketing service offerings among the categories of service (i.e., local, interexchange, and CMRS) to which the customer already subscribes from the same carrier, without customer approval.

DLS will not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

DLS may use, disclose, or permit access to CPNI, without customer approval, in its provisioning of inside wiring installation, maintenance, and repair services.

DLS may use CPNI, without customer approval, to market services formerly known as adjunct-to-basic services, such as, but not limited to, speed dialing, computer-provided directory assistance, call monitoring, call tracing, call blocking, call return, repeat dialing, call tracking, call waiting, caller I.D., call forwarding, and certain centrex features.

DLS may use, disclose, or permit access to CPNI to protect DLS' rights or property, or to protect users of those services and other carriers from fraudulent, abusive, or unlawful use of, or subscription to, such services.

**Safeguards used for customers proprietary network information**

It is a policy of DLS to restrict sales and marketing teams security access to the customer's account information in order to prevent them from accessing CPNI. Explicit mandatory annual training program for Sales and Marketing teams is in place to ensure compliance with this policy.

**Disclosure of Customers Proprietary Network Information**

Safeguarding customer proprietary network information for VoIP customers:

CPNI including call detail information may be provided to a customer on a customer-initiated call or store visit only after they provide their account password or a valid photo id matching their account information. If the customer is unable to provide an account password or valid photo id, CPNI information may only be provided by calling the customers telephone number of record or by sending the information to the mailing address of record (postal or email).

If a customer is unable to verify their password or present a valid photo-id, a new password can be established by placing a call to the customer's telephone number of record and speaking with the account holder.

Whenever a password, telephone number of record or address of record is changed, a notification must be sent to the customer at their address of record (postal or email) including the following statement: "The telephone number, address, or password for this account has recently been changed. If you did not authorize this change, please contact us immediately." The notice must not contain the specific information that was changed or what it was changed to. If an address of record was the item changed, the notice must not be sent to the new address.

**Notification of customer proprietary network information security breaches.**

1. Definitions. A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI.
2. DLS Network Operations Team will notify law enforcement of any breach of the database containing CPNI as soon as practical and no later than within 7 business days of the breach. The following law enforcement agencies will be notified electronically via FCC reporting facility at <http://www.fcc.gov/eb/cpni/> :
  - United States Secret Service (USSS)
  - Federal Bureau of Investigation (FBI)

DLS Network Operations Team is also required to notify DLS management, sales and customer service teams of the incident as soon as practical.

3. DLS Customer Service representative will wait at least 7 working days since the time appropriate law enforcement agencies have been contacted prior to notifying its customer via electronic and postal mail about any breach of a system containing CPNI.
  - a. DLS will cooperate with the relevant investigating agency's request to minimize any adverse effects of such customer notification.
4. If the relevant investigating agency determines that public disclosure or notice to customers would impede or compromise an ongoing or potential criminal investigation or national security, at the direction of the investigating agency DLS Network Operations team is not to so disclose or notify for an initial period of up to 30 days. Such period may be extended by the agency as reasonably necessary in the judgment of the agency. If such direction is given, the agency must notify DLS when it appears that public disclosure or notice to affected customers will no longer impede or compromise a criminal investigation or national security. The agency shall provide in writing its initial direction to DLS, any subsequent extension, and any notification that notice will no longer impede or compromise a criminal investigation or national security and such writings shall be contemporaneously logged on the same reporting facility that contains records of notifications filed by carriers (<http://www.fcc.gov/eb/cpni/>)
  - a. DLS may forgo the 30 day waiting period if there in the event of strong evidence that such delay may be causing an immediate and irreparable harm. DLS Network Operations Department will so indicate in its notification and may proceed to immediately notify its affected customers only after consultation with the relevant investigating agency.
5. All records of interaction between DLS and law enforcement agencies as well as records of interactions between DLS and the customer with regard to a breach of CPNI information is to be filed with the DLS accounting office and will be stored for 4 years. The record must include, if available, dates of discovery and notification, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.